Pattern Recognition 45 (2012) 3373–3388

Contents lists available at SciVerse ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs

Priyanka Das [a], Kannan Karthik [a,*], Boul Chandra Garai [b]

[a] Dept. of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, India
[b] ISRO Satellite Centre, Bangalore, India

ARTICLE INFO

Article history:
Received 23 May 2011
Received in revised form
20 January 2012
Accepted 26 February 2012
Available online 9 March 2012

Keywords:
Fingerprint
Hash
Minimum distance graph
Corresponding search algorithm
Security

ABSTRACT

Abstraction of a fingerprint in the form of a hash can be used for secure authentication. The main challenge is in finding the right choice of features which remain relatively invariant to distortions such as rotation, translation and minutiae insertions and deletions, while at the same time capturing the diversity across users. In this paper, an alignment-free novel fingerprint hashing algorithm is proposed which uses a graph comprising of the inter-minutia minimum distance vectors originating from the core point as a feature set called the minimum distance graph. Matching of hashes has been implemented using a corresponding search algorithm. Based on the experiments conducted on the FVC2002-DB1a and FVC2002-DB2a databases, we obtained an equal error rate of 2.27%. The computational cost associated with our fingerprint hash generation and matching processes is relatively low, despite its success in capturing the minutia positional variations across users.

1. Introduction

Biometric authentication system is divided into two stages—(i) enrollment: to extract the features from the scanned biometric data of the user, create a template, and store it in the database, and (ii) authentication: to extract the same features from the query user's biometric data and compare the result with the stored template. If they are sufficiently similar according to some similarity measure, the matching module output is YES, indicating an authentic user, or a NO for an unauthorized user.

Since it is extremely difficult to replace or revoke the biometric data, the user biometric data must be kept in a secure way when used for authentication. So, instead of storing the raw biometric data in the database, it is preferable to store corresponding transformed versions, so that (i) they can still be used for matching with reasonable performance and (ii) it would be hard to forge the "original" biometric data that would match a given template. One possible way is to generate robust hash functions. The hash function should be such that it will give similar hash values for the same user and completely different hash values for different users.

A fingerprint based biometric is commonly used to authenticate a genuine user due to three primary reasons: its universality, distinctiveness and permanence. But fingerprint matching is a difficult problem due to large *intra-class variations* such as, displacement, rotation, partial overlap, non-linear distortion, pressure and skin conditions, noise, etc. The global structures (position of singularity, local ridge orientation) of fingerprint images from different users may sometimes look similar causing large *inter-class similarity*. A fingerprint consists of ridges and valleys which carry a lot of information and form a set of distinctive features for a wide class of users. Two most prominent local ridge characteristics are ridge ending and ridge bifurcation collectively known as minutia.

In this paper, we devise a novel fingerprint hashing algorithm called the Minimum Distance Graph (MDG) generated for both query and template image with the help of singular point (core) and minutiae points. Maximum number of matching pairs between the query MDG and template MDG are found with the help of our Corresponding Search Algorithm (CSA). In the first phase of CSA, we find a maximum set of matched node pairs from the two distance vectors, and in the second phase, we include more pairs in the match by comparing the rest of the elements of these two vectors. The pre-alignment phase is not required in our algorithm. The results are presented to demonstrate significant improvements in fingerprint matching accuracy through the public fingerprint databases FVC2002-DB1a, FVC2002-DB2a.

The rest of the paper is organized as follows. In Section 2, we present a brief discussion of some recent work in the area of transformed anonymous biometrics for secure fingerprint authentication. Section 3 deals with pre-processing, reference point detection, minutiae extraction and false minutiae removal steps. We describe our MDG hashing algorithm in detail in Section 4.

* Corresponding author. Tel.: +91 361 2582516; fax: +91 361 2582542.
E-mail addresses: d.priyanka@iitg.ernet.in (P. Das), k.karthik@iitg.ernet.in (K. Karthik), bgarai@isac.gov.in (B. Chandra Garai).

0031-3203/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2012.02.022

How the hashing algorithm really qualifies as a robust fingerprint perceptual hash is discussed in Section 5. Section 6 is related to the determination of maximum matching pairs using the corresponding search algorithm. Security issues are discussed in Section 7. Experimental results, comparison with other hashing methods and complexity analysis are presented in Section 8. In Section 9, we have described how our hashing algorithm can be extended to generate cancelable templates. Finally, in Section 10, the conclusions are presented.

2. Related work

Most template protection approaches can be roughly classified into two categories: (i) transformation based and (ii) biometric cryptosystems. In the first case, the matching between template and query image is performed in transformed domain. So, leakage of original biometric information is not possible. It is very challenging to find an optimal transformation that is non-invertible, while preserving matching accuracy. One way to do this is by using robust, non-invertible hash functions.

A fair amount of attention has been directed towards hash function based fingerprint authentication. A secure biometric authentication scheme based on robust hash function has been proposed by Sutcu et al. [1]. A combination of various Gaussian functions with a secure cryptographic hash function is used in their paper to satisfy both non-invertibility and security conditions. An efficient distortion tolerant fingerprint authentication scheme has been presented in [2] based on labeled and weighted graphs of minutiae features known as the Minutiae Adjacency Graph (MAG). Generation of cancelable template using cartesian, polar and surface folding transformations from minutiae points has been shown by Ratha et al. [3]. The registration prior to transformation has been accomplished by the position and orientation of the core point in their method. Lee et al. have described an alignment-free cancelable fingerprint template generation method based on local information around each minutia [4]. For each minutia, the rotation and translation invariant value is computed from the orientation information of local region close to the central minutia. Another novel method to generate cancelable templates by Bin-based Quantization (BQ) has been proposed by Yang et al. [5]. They have used both local and global fingerprint features for better discrimination between users.

Application of a family of symmetric hash functions for secure fingerprint biometric systems appears in the work of Tulyakov et al. [6]. The algorithm does not depend on the singular points (core and delta) and does not need pre-alignment between the test and reference fingerprint templates. They have extended their work by generating a combination of symmetric hash functions in order to enhance the security of the system against brute force attack [7]. The advantage of this approach is that the algorithm is applicable to partial fingerprint matching without requiring pre-alignment. Yang et al. [8] presented a dynamic random projection-based template protection algorithm which increases the computational complexity to search for the original unprotected biometric template when the bio-token is stolen. Yang and Busch [9] developed a parameterized geometric alignment method for fingerprint template protection. In this method, minutiae vicinity is defined by each minutia itself together with M closest neighbouring minutiae. The main idea is to infuse randomness into the minutiae vicinity self alignment process in order to achieve template diversification.

Lee and Kim [10] used minutiae-based bit strings as cancelable templates. Firstly a three-dimensional array consisting of cells is generated. A reference minutia point is selected and other minutiae are translated and rotated in order to map the minutiae into the cells and a one-dimensional bit-string is generated. Finally, the bit-string is permuted using user specific PIN or the permutation matrices. This approach performs well when all the users have different PINs, however the performance degrades when the key is compromised due to quantization error and image distortion. Another bit-string based cancelable template generation method appeared in the work of Jin et al. [11]. In their method, a set of invariant features are extracted from minutiae pairs, and further they apply quantization, histogram binning and binarization operations to generate a bit-string. Finally the bit-string is transformed into a non-invertible and cancelable one using helper data and user's key based permutation procedure. But how the minutiae pairs are to be chosen is not mentioned in their paper. Farooq et al. [12] presented an alignment-free cancelable template generation method based on minutiae triplets (triangles). The authors have extracted seven invariant features followed by quantization and hashing into a binary string (2^{24} bits). However the computational complexity of this method is high as calculation of all possible triplet invariant features are required. Another registration-free cancelable template design method is proposed by Ahmad et al. [13]. The authors have designed pair polar coordinate space where relative position of a minutia point with respect to other minutiae points is computed. Matching process is performed in transform domain to satisfy the property of non-invertibility.

A fully automated and practical fuzzy vault scheme based on fingerprint minutiae has been proposed by Nandakumar et al. [14]. Their method strongly depends on the alignment accuracy. The authors have used high curvature points derived from orientation field as helper data for alignment which leaks sufficient information to the attackers. In addition, due to non-linear deformation in fingerprints, the high curvature points cannot be reliably obtained in certain images and this leads to a slight misalignment. An improved minutiae descriptor (ridge frequency and ridge orientation) based fuzzy vault scheme is presented in [15]. However, their approach also relies on alignment accuracy. Liu et al. [16] have proposed a key binding system using n-nearest minutia structures. They have demonstrated that fingerprint matching performance can be improved substantially by incorporating more genuine points in the vault, but which in turn, increases the computational complexity.

In summary, it is extremely difficult to develop a fingerprint authentication algorithm which satisfies the conditions of high matching accuracy, low computational complexity and more security simultaneously. This is the motivation of our paper.

3. Pre-processing

The complete hashing algorithm is shown in Fig. 1 in the form of a block diagram. Each block is discussed below.

3.1. Fingerprint image enhancement

The first step of any fingerprint matching process is to enhance both the template and query fingerprint images. Different approaches are implemented in spatial domain or frequency domain to reduce noise and to increase the contrast between ridges and valleys in the gray-scale fingerprint images before further processing. Given a fingerprint image, the Gabor filtered based enhancement algorithm proposed by Hong et al. [17] is adopted to obtain the enhanced binary fingerprint image. The main steps are

- Normalization.
- Segmentation.
- Orientation image estimation.
- Ridge frequency image estimation.